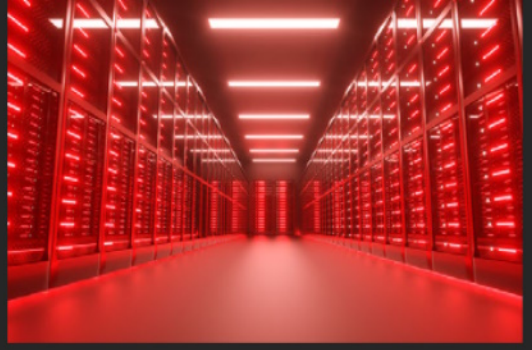
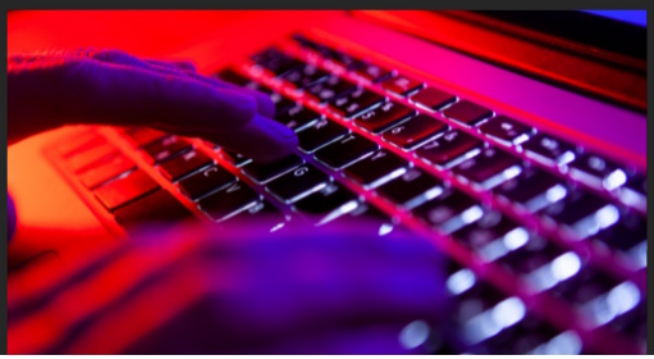




Security Assessment

Quote # 022123
Version 1

Prepared for:

Village Of Orland Park

Tad Spencer
tspencer@orlandpark.org

Fortis Non-Recurring Pricing

Description	List Price	Discount	One-Time Price
Fortis™ Cyber Advisory Services - Security Assessment Services • Strategic Security Assessment: Included	$51,627.50	20.00%	$41,302.00
		Subtotal:	**$41,302.00**

Fortis Statement of Work - Cyber Advisory

Security Assessment

Executive Summary

Village of Orland Park has engaged Sentinel to provide an assessment of the current security infrastructure and provide recommendations that are based on a strategic approach.

The strategic assessment approach aligns organizational goals and objectives with technology recommendations. Sentinel will meet with key organization stakeholders to gain insight into current challenges as well as future initiatives. This process will provide guidance for the analysis and recommendation phases of the engagement. Sentinel will gather information about the current security infrastructure, topology, devices, and configuration to review it for technical best practice adherence and alignment with organizational goals. A prioritized list of recommendations will be presented to the organization and linked to the key initiatives that are defined in prior phases.

The goal of the assessment is to provide a comprehensive analysis and objective review of the current implementation and provide insight into any future changes that should be made. Although assessments will cover all areas outlined in this proposal, the following areas will be specifically focused on as part of the engagement:

- ~ 1000 devices.
    - Vulnerability scanning.
- NIST Cybersecurity Framework alignment.
- Stakeholder interviews.

Additional focus on CJIS & PCI requirements. Though not a dedicated review of each regulation, this will provide visibility into the potential gaps for these regulations outside of NIST CSF requirements.

As a follow-up to the assessment engagement, Sentinel can provide remediation services for those objectives the customer wishes to pursue and remediate further. Sentinel appreciates the opportunity to provide these services to Village of Orland Park and looks forward to reviewing the results with the team.

Security Assessment Approach

The assessment will provide actual (as-built) documentation, analysis, and recommendations. Sentinel follows a multi-phased approach with assessments as outlined below:

Fortis Statement of Work - Cyber Advisory

Phase One – Gather

Fortis Statement of Work - Cyber Advisory

The first phase of the assessment is an information gathering engagement that will provide detailed information about the current environment including both technical and non-technical data. For strategic assessments, Sentinel will meet with the customer stakeholders through an interview session to gather key objectives and goals for the organization. This information will be used to provide perspective and influence on the analysis and recommendations in later phases of the assessment.

A solid security plan goes beyond technology and addresses the entire cybersecurity lifecycle of an organization. During the stakeholder interview session(s) a Sentinel Strategic Advisor will review the National Institute of Standards and Technology (NIST) Cybersecurity Framework with the customer and review organizational alignment to these standards. The NIST Cybersecurity framework provides a comprehensive approach to protecting critical infrastructure using standards and guidelines. This framework emphasizes a prioritized, flexible, repeatable, and cost-effective approach for organizations manage cybersecurity-related risk.

Technical information will be gathered using the existing access credentials to perform a discovery with custom Sentinel tools and manual efforts. The documentation produced by Sentinel will include connectivity information about the infrastructure as well as any additional information discovered for ancillary devices. This documentation provides the baseline information needed by the Sentinel team to analyze the respective technology areas in future phases of the engagement.

Phase Two – Analyze

The second phase of the assessment includes a thorough analysis of the collected information from phase one and performs a technical gap analysis between the current implementation and a best practice implementation in several categories. Both strategic and tactical analysis options are outlined below.

Strategic Analysis

Fortis Statement of Work - Cyber Advisory

The strategic analysis identifies actionable items that factor in to the customer's organizational requirements, objectives, and goals. This option allows the recommendations to be tailored for the customer, providing influence and perspective in other areas such as growth, performance, and resiliency, using a holistic approach to ensure the most reliable and functional environment possible. Stakeholder interviews will be performed during the information discovery phase to identify the goals and objectives that will influence the analysis and subsequent recommendations in the final phase of the assessment.

Sentinel will work with the customer to help identify any gaps between the current organizational security approach and those defined by NIST and industry best practices. Cybersecurity policies and procedures will be reviewed and compared to industry best practices to identify any potential compliance or audit exposure for the organization. One of the most vulnerable areas in an organization is its employees. Many users are unaware of proper security policies and procedures when it comes to utilizing company infrastructure. As an optional component to the strategic assessment approach Sentinel can provide planned phishing attacks against the customer organization to determine whether additional policy development is necessary as well as user education.

Tactical Analysis Categories

Fortis Statement of Work - Cyber Advisory

Phase Three – Recommend

The third phase of the assessment is where Sentinel will provide a prioritized list of recommendations based on the analysis performed during phase two of the assessment. For tactical assessments, the recommendations will not be influenced by organizational goals and objectives and are considered a subjective opinion based on general industry practices. The strategic assessment recommendations will be influenced and evaluated based on customer organizational goals and objectives gathered during phase one. Findings will be prioritized based on business impact, likelihood, and risk, to determine overall priority.

Sentinel services during this phase may include, but are not limited to the following:

- Strategic Assessments.
  - Organizational alignment to goals and future state objectives.
  - Overall constraints, budgets, non-technical influences.
  - Security deficiency identification with recommendations.
  - Identifying ideal software versions with bug and security vulnerability awareness.
  - Configuration standardization with best-practice consistencies.
  - Recommended configuration changes.
  - Software/hardware upgrade recommendations.

Scope of Work

Phase One - Information Gathering

Process

- Strategic Assessments
  - Work with the customer to determine the appropriate stakeholders that will be interviewed.

- Provide the stakeholders with a pre-interview overview of the question topic.
- Perform an on-site or remote interview session with key customer stakeholders to gather information regarding organizational goals and objectives.
- Review the NIST Cybersecurity Framework, and Customer cybersecurity policies.
- Review the items within scope for the assessment with the customer to ensure agreement and any additional information, comments, or concerns about the environment.
- Sentinel will perform remote data collection on the infrastructure components considered in scope for the respective technology areas. This may include applications, devices, services, etc. depending on the environment.
    - Remote data collection is the Sentinel preferred method of collection, and will be performed via remote VPN (or equivalent) with access to all infrastructure components and segments under assessment. If remote access is not feasible due to customer security requirements or capabilities, on-site data collection can take place using Sentinel specific tools loaded on Sentinel provided equipment. Sentinel on-site engineer is available upon request and quoted separately.
- Sentinel will require access to all scoped infrastructure with appropriate credentials.
- Sentinel will utilize various custom and commercial tools to collect infrastructure information.
    - The tools may require that a Sentinel Virtual Appliance (SVA) be deployed for local data collection (i.e. security vulnerability scanning, traffic analysis/polling, Netflow, SNMP, etc.).
    - Sentinel Virtual Appliance (SVA) will typically remain on customer premise for a standard duration of at least two (2) weeks however, time may vary based on the assessment scope.
- Sentinel will identify a list of inaccessible devices for the customer to remediate or be excluded from the assessment documentation.
- Sentinel will typically run a final scan after all infrastructure components are accessible.

Sentinel Deliverables

- Strategic Assessments.
    - Stakeholder goals and objectives gathered during interview sessions.
    - Security policies and procedures information.

Customer Responsibilities

- Strategic Assessments.
    - Determine appropriate organization stakeholders that should participate in the stakeholder interview sessions. This will include both technical and non-technical participants.
        - Provide employee list and contact information.
    - Provide access to security policies and procedures.
    - Participate in stakeholder meetings to gather appropriate organizational information.
    - Provide VPN (or equivalent) access for remote data collection. If remote access is not available to Sentinel, provide on-site access to customer network via Sentinel owned device. On-site Sentinel engineer available upon request and is quoted separately.
    - Provide access to all infrastructure devices under assessment including credentials (username/pwd).

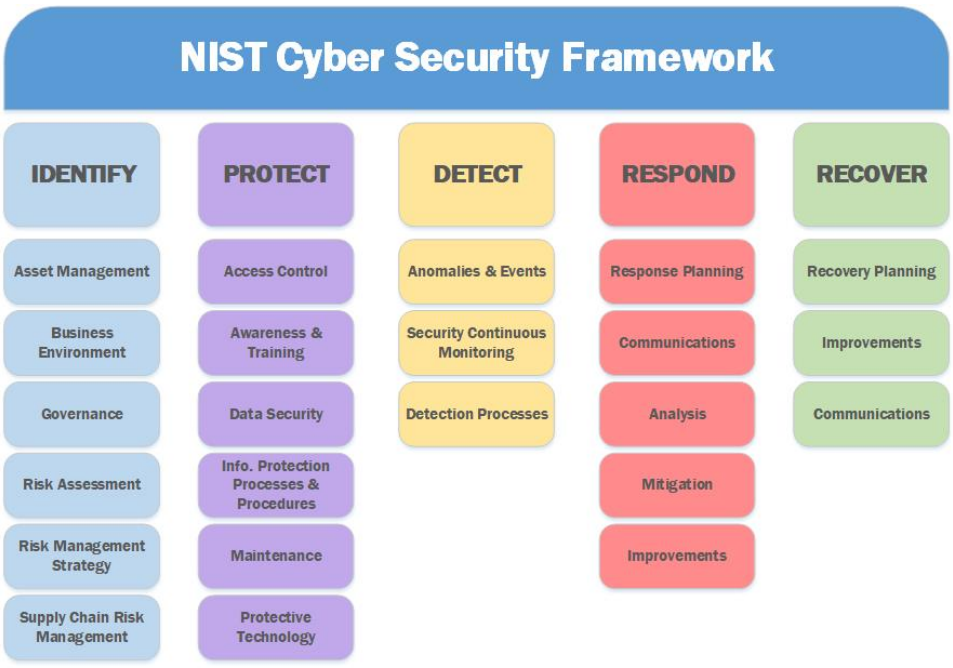
- Tools will require IP connectivity, admin level credentials, and management access (I.e. Telnet, SSH, SNMP, etc.) for onsite or remote VPN facilitated methods.
- For security assessments SPAN ports may be required for traffic analysis. (I.e. Internet edge, server vlan, etc.) RSPAN may be used where possible and technically feasible.
- Tools may require host-based security reporting software to be installed on client/server.

- Complete any device access remediation. Sentinel support available and quoted separately.
- Provide any relevant maintenance status/contract information to assist with information gathering.
- Participate in meetings to review documentation results.

Phase Two – Analysis

Process

- Strategic Assessments.
  - This includes a broader conversation around the infrastructure as a whole and includes a deeper analysis of the customer requirements based on organizational goals.
  - Sentinel will perform a technical gap analysis between the current environment and the desired goals and objectives. A priority weighting will be performed based on organization impact, likelihood of occurrence, and risk for each recommendation.
  - Sentinel will document recommendations and tailor them to meet the customer's identified goals and objectives where applicable.
  - A broader in scope conversation around the NIST Cybersecurity Framework will be performed as well as a deeper analysis of the customer's security posture.
  - Sentinel will review collected policies to and identify areas of improvement and/or compliance concerns.



- Sentinel utilizes information gathered in phase one to identify design, configuration, and code-specific (security vulnerabilities) issues/errors to make recommendations which are intended to improve reliability, stability, and/or performance.
- Sentinel will perform a technical analysis on a per-device or logical grouping basis. This analysis will be documented as part of the deliverable document in a findings section organized by infrastructure type and category. Findings will rated based on business impact, likelihood of occurrence, priority/risk, and complexity.

Sentinel Deliverables

- Sentinel will provide a summary of the analysis findings in a prioritized listing. This document will identify issues that were observed during the information gathering and analysis phases of the assessment. These findings will be used to develop the prioritized list of recommendations based on category. Priority will be weighted based on organizational goals and objectives for strategic assessments. For tactical assessments the priority will be a subjective opinion based on Sentinel and industry practices. The analysis will be based on several areas including the following:
  - Strategic Assessments.
    - Stakeholder interview session goals and objectives summary.
    - Technology alignment with the organizational direction and focus.
    - Future project impact, timelines, milestones, and goals.
    - Best practice design, configurations, and deployment methodologies.
    - Planned and organic growth, scalability, etc.
    - Security vulnerability report.

Customer Responsibilities

Participate in any meetings to review documented findings.

Phase Three – Recommendations

Process

- Sentinel will utilize the findings from the analysis phase to provide a prioritized list of recommendations.
- Each recommendation will include background information on the topic being discussed in order to provide context for the technical recommendation to follow. Recommendations may reference industry or manufacturer best practice documentation as well as suggested high-level remediation steps.
- Recommendations will be aligned with organizational goals and objectives as part of a strategic assessment and for tactical assessments, provided based on Sentinel opinion and industry practices.
- Supplemental documentation may be provided for customer reference and additional supporting documentation for topic areas.

Sentinel Deliverables

Fortis Statement of Work - Cyber Advisory

Sentinel will provide a prioritized list of recommendations to the customer based on the analysis findings.

Customer Responsibilities

Participate in meetings to review documented recommendations.

Project Management

Sentinel will provide a project manager committed to the success of the project. The project manager will be responsible for:

- Complete success of the project.
- Optimal coordination of all resources.
- Guiding the customer on aspects of the project they are required to perform.
- Tracking and reporting of progress.
- Management of expected timelines for the assessment.
- Changes to the project and communications of changes in writing using a Sentinel Change Order.
- Post-assessment project completion agreement and signature.

Project management will ensure complete project success. Communication is the cornerstone of project management and the project manager will be the central communication mechanism for all parties. This will assure all relevant parties are informed about decisions that may affect the success of their component of the solution.

General Assumptions

The following is a list of general project assumptions which Sentinel assumes have been completed or reviewed by the customer prior to the start of the project.

- Sentinel guarantees that it will perform any tests in a responsible and professional manner in accordance with best practices and that it will use its best efforts not to change or amend any applications, data, programs, or components of the Customer's network (including hardware and software). This does not guarantee against any disruption or effect on the Customer's production systems. The Customer understands that Sentinel shall not be liable for any damages that may arise from any such disruption.
- The current infrastructure under assessment is in an operational state, excluding any specific issues that may be under evaluation as part of the assessment services. Sentinel has not included any troubleshooting or remediation services as part of this proposal.
- The Customer has access to all infrastructure areas under assessment and can provide this information to Sentinel. **Note: Service provider managed equipment may not be accessible and therefore excluded from assessment unless configuration(s) can be provided by the customer.**
- Sentinel assessment services are performed **remotely** utilizing customer provided remote access. If on-site services are desired or required, they can be quoted separately including any applicable travel costs.
- Any information discussed and/or provided by Sentinel to the customer is considered confidential and should not be distributed outside the customer's organization without Sentinel's written approval.
- Remediation of any assessment recommendations are not included within this proposal and can be quoted separately.

Security Assessment

Prepared by:

Sentinel Technologies, Inc

Dan Shea
dshea@sentinel.com

Prepared for:

Village Of Orland Park

14700 S Ravinia Ave
Orland Park, IL 60462-3134
Tad Spencer

tspencer@orlandpark.org

Contract Information:

Contract #: 022123

Version: 1
Delivery Date: 05/07/2025
Expiration Date: 05/25/2025

Quote Summary

Description	Amount
Fortis Non-Recurring Pricing	$41,302.00

Fortis™ Cyber Advisory Services

Fortis™ Cyber Advisory Services - Security Assessment Offerings	FORTIS CYBER ADVISORY		

Strategic Security Assessment
• Included devices (Workstations, Servers, Cameras, Printers, IoT devices, etc.)
  ◦ Internal vulnerability Scanning
  ◦ Single device deployment
  ◦ Stakeholder interviews
  ◦ NIST Cybersecurity Framework
  ◦ PCI
  ◦ CJIS
	Included	**#Devices**	1000